September 12, 2017, 4:00 AM GMT+8 Updated on September 12, 2017, 7:53 AM GMT+8

North Korea Is Dodging Sanctions With a Secret Bitcoin Stash

Yuji Nakamura and Sam Kim

North Korean hackers target South Korea's ethereum exchanges

Crypto-currencies become tool to raise and launder money

North Korea appears to be stepping up efforts to secure bitcoin and other cryptocurrencies, which could be used to avoid trade restrictions including new sanctions <https://www.bloomberg.com/politics/articles/2017-09-11/un-votes-new-north-korea-sanctions-stopping-short-of-oil-embargo> approved by the United Nations Security Council.

Hackers from Kim Jong Un's regime are increasing their attacks on cryptocurrency exchanges in South Korea and related sites, according to a new report <https://www.fireeye.com/blog/threat-research/2017/09/north-korea-interested-in-bitcoin.html> from security researcher FireEye Inc. They also breached an English-language bitcoin news website and collected bitcoin ransom payments from global victims of the malware WannaCry <https://www.bloomberg.com/politics/articles/2017-05-12/patients-turned-away-as-british-hospitals-hit-by-cyber-attack> , according to the researcher.

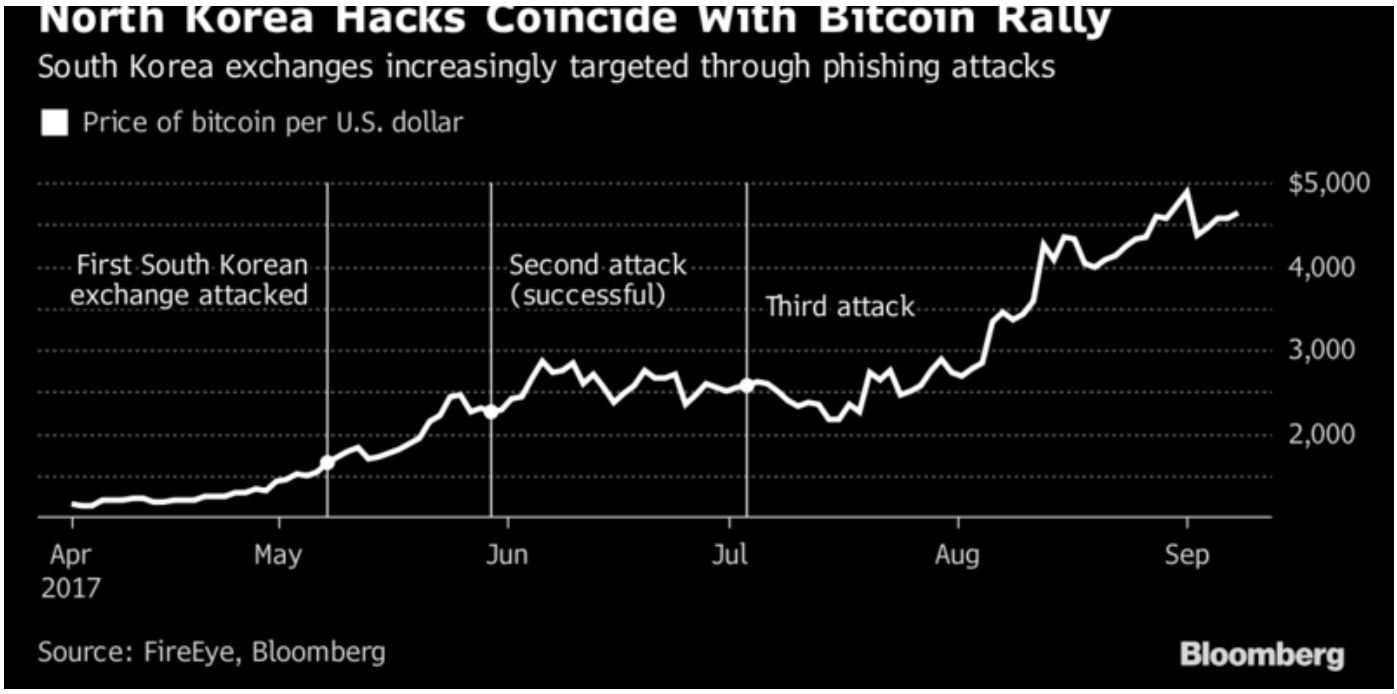
Kim's apparent interest in cryptocurrencies comes amid rising prices and popularity. The same factors that have driven their success -- lack of state control and secretiveness -- would make them useful fund raising and money laundering tools for a man threatening to use nuclear weapons against the U.S. With tightening sanctions and usage of cryptocurrencies broadening, security experts say North Korea's embrace of digital cash will only increase.

"We definitely see sanctions being a big lever driving this sort of activity," said Luke McNamara <https://www.linkedin.com/in/lukemcnamara/> , a researcher at FireEye and author of the new report. "They probably see it as a very low-cost solution to bring in hard cash."

The 15-member Security Council on Monday approved sanctions <https://www.bloomberg.com/politics/articles/2017-09-11/un-votes-new-north-korea-sanctions-stopping-short-of-oil-embargo> aimed at punishing North Korea for its latest missile and nuclear tests. U.S. officials said the new measures would cut the country's textile exports by 90 percent, restricting its ability to get hard currency.

So far this year, FireEye has confirmed attacks on at least three South Korean exchanges, including one in May that was successful. Around the same time, local media reported that Seoul-based exchange Yapizon lost more than 3,800 bitcoins (worth about $15 million at current rates) due to theft, although FireEye said there are not clear indications of North Korean involvement.

North Korea's telecommunications ministry didn't respond to an emailed request for comments. The country's diplomats and official media have denied the country played any role in cyberattacks, including the hacking of Sony Pictures Entertainment in 2014.



North Korea operates what South Korea believes is an army of hackers expanding its focus from military espionage to financial theft. The regime's Reconnaissance General Bureau, which directly reports to Kim Jong Un, handles peacetime cyber operations from espionage to network disruptions and employs an estimated 6,000 officers, according to a 2016 report from the International Cyber Policy Centre at the Australian Strategic Policy Institute.

In the recent round of attacks, South Korea may have become a target not just due to its proximity to Pyongyang and shared language, but because the country has become one of the busiest trading hubs for cryptocurrencies this year. Seoul-based Bithumb is the world's biggest exchange for ethereum. In June, it said hackers had stolen customer information from an employee's computer, without identifying the attackers.

"As more money goes into cryptocurrency exchanges and more people buy bitcoin and ethereum, exchanges become larger targets for this group," said McNamara. He said so far he did not have evidence that Kim Jong Un's regime has targeted cryptocurrency exchanges outside of South Korea, but did not rule out the possibility in the future.

Besides exchanges, FireEye said an English-language bitcoin news website was breached by North Korea, which would likely allow hackers to identify people visiting the site. It declined to name the website and said it believes North Korea prefers larger targets like exchanges than individual owners of cryptocurrencies.

The firm said previously <https://www.bloomberg.com/news/articles/2017-05-23/cybersleuths-unearth-more-clues-linking-wannacry-to-north-korea> it had found a connection between Pyongyang and the WannaCry attack from May and June, which affected more than 300,000 computers worldwide. McNamara said he also sees indications North Korean hackers are getting involved in cryptocurrency mining.

Attacks on the South Korean exchanges were carried out through so-called spear-phishing attacks, or emailing files laced with malware to specific targets. FireEye identified the malware, known as PEACHPIT, and provided examples of documents it was attached to, including one published by Seoul-based Hyundai Research Institute about the state of bitcoin industries. When contacted, the author of the report confirmed he wrote it in 2014, but was unaware that someone was distributing a press release about it this year.

The group behind the hacks, which FireEye identified as TEMP.Hermit, has made a name for itself out of bitcoin theft, including a 2015 attack on South Korea's nuclear industry. The hackers have also been tied <https://www.wired.com/2016/02/evidence-suggests-the-sony-hackers-are-alive-and-well-and-still-hacking/> by other security firms to last year's attack on Samsung Electronics Co.'s corporate messenger app and, most prominently, the breach of Sony Corp.'s film studio, which the FBI blamed <https://www.fbi.gov/news/pressrel/press-releases/update-on-sony-investigation> on North Korea.

"They're pretty capable actors in comparison to other North Korean activity we see," said McNamara. "They've been creative in how they use their cyber-espionage capability."

The malware used in bitcoin hacks is linked to the group suspected of attacks on the payment systems of global banks last year, according to FireEye. The FBI is also examining North Korea's link to the theft of $81 million through the New York Fed last year, Bloomberg Markets reported last month.

FireEye said if the hackers wanted to convert bitcoin or ethereum into dollars or won, they'd likely first exchange them into harder-to-trace <https://www.bloomberg.com/news/articles/2016-08-29/new-digital-currency-spikes-after-giving-criminals-more-secrecy> cryptocurrencies like Monero and then into fiat currency. A similar technique was used last month to empty <https://www.bloomberg.com/news/articles/2017-08-03/wannacry-linked-bitcoin-wallets-have-been-emptied-analysts-say> the bitcoin wallets related to WannaCry.

▲ A Look Inside One of the World's Biggest Bitcoin Mines

"They could compromise an exchange and transfer those bitcoins to other exchanges elsewhere in Asia or exchange them for a more anonymous cryptocurrency," said McNamara. "There are variety of things they could do to cash out."

Watch Next: A Look Inside One of the World's Biggest Bitcoin Mines

▲